1026 Addison Street
Berkeley, CA 94710-2137

September 6, 2000

Ms. Magalie R. Salas
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Ms. Salas:

Re: The Motion Picture Association of America's comments of 25 August, 2000 on PP Docket No. 00-67.

There most certainly *is* evidence that content owners will restrict time-shifting and other fair use of content delivered to households. Certain content owners and their agents are currently engaged in litigation against fair use, *c.f.* the cases of:

- Universal City Studios, *et al.* v. 2600 Enterprises in New York,
- Universal City Studios, *et al.* v. Hughes in Connecticut, and
- DVD Copy Control Assoc. v. McLaughlin, *et al.* in California.

More information on these cases is available at `http://eon.law.harvard.edu/openlaw/DVD/`. These cases are seeking to enjoin individuals from participating in scholarly research using digial media.

The owners as represented by the MPAA state that they would allow such uses if people would ask, but they have no public procedures in place for obtaining the correct permission and utilities. And what if the content owners think that the research might portray them in a poor light, as in research linking portrayals of entertainment violence to incidents of youthful violence? Will they still allow the research to proceed, or is this why there seem to be no procedures to allow such research with digital media?

Some excellent examples of the types of research impacted by similar copy protection schemes have been outlined by Drs. Appel and Felten in comments to the Copyright Office of the Library of Congress. The comments also have been published in this month's *Communications of the ACM* (Sept. 2000, vol. 43, no. 9, pp. 21-23, also available on-line). Please examine those comments and consider the current litigation as evidence that significant content owners *will* use the technologies to defeat fair use. *This* is the "actual conduct of content owners" (third paragraph of the MPAA *Ex-Parte* letter of 25 Aug., 2000).

The owners' actions against fair use already call into question their motives behind pushing a particular copy protection scheme onto consumers. An FCC mandate enforcing this scheme will destroy long-term interoperability and will cripple very promising alternative technologies.

Consider the impact of overzealous copy protection hardware on interoperability. While mandating one or a few set copy protection schemes will solve the interoperability problem for the short-term, it fails as a long-term solution. As soon as these schemes are defeated, all extant equipment will be rendered obsolete. New digital media will no doubt require new players, raising the interoperability problem again and again. Also, any new equipment will need to support all old copy protection schemes, assuming supporting fair-use archival is within the manufacturer's best interests. This will not only bring interoperability back before the FCC every few years but will also cause consumers to replace expensive equipment much more often than they currently do.

All digital copy protection schemes will be defeated. There is a long history of this for quite simple reasons. All digital signals, both digital and analog, must be presented to a human viewer in a clear, analog form. A full copy protection scheme for digital media must combine the transformation from a protected signal into a clear one with the transformation from a digital signal into a perceptual, analog one, or it would be trivial to intercept the signal between the two transformations. Many copy 'protection' schemes fail to recognize that and fall to trivial analysis. More complex schemes must mix the two stages in the same integrated units, and that provides a relatively easy target for reverse engineering and cryptanalysis. It also provides an easy unit to replace once the analysis is completed, enabling easy modifications to defeat copy protection.

Obviously, this leads to a war of implementation complexity. The more complex the implementation, the longer it withstands analysis, but the time scales are drastically different. The complex implementation may take five years and millions of dollars, while the analysis may take two months in spare time. This is a race that cannot be won, and consumers will bear the burden of paying for it. They must both fund the development of the changing implementations through higher prices and fund the changing FCC regulations governing interoperability through taxes.

Is there a better way? Perhaps. Consider the potential problems with excellent color photocopiers. With very little effort, people should be able to manufacture false identification and forge counterfeit money. Indeed, this has happened, but the parties involved have met with a rude shock. Photocopiers embed identification tags in their output through watermarking. The watermarking has allowed enforcement of existing laws without disturbing fair use principles. Limiting the identifying watermark to the photocopier rather than associating it directly with the photocopier user also protects user privacy from cursory invasions.

Photocopiers are considered analog devices, but the watermarking concept can

also carry over to digital media. You can find more information about digital watermarking through the links available at `http://www.cl.cam.ac.uk/~fapp2/steganography/`. These watermarks are secure against reasonable degredations of the digital signal. Once the signal degrades far enough to destroy the watermark, it is no better than a poor analog reproduction. Such poor reproductions are already possible and do not seem to impact the content producers overmuch.

Digital watermarking could provide a method for content owners to enforce copyright without restricting fair use, assuming that a watermark can be associated with the digital media sent to an individual. There are a few options on where in the media stream to insert the watermarking:

- on the consumer's end,
- on the producer's end, and
- within the distribution network.

The easiest would be to insert the watermark on reception in the consumer's unit. This would be vulnerable to many of the same attacks that apply to copy protection hardware. However, the watermarking will not inconvenience the end user, so the user will be much less likely to spend money and effort on modifications. There are also fewer interoperability concerns. The watermarking process is essentially transparent to recording and playback, so most equipment need never change even when watermarking standards are changed. Indeed, the watermarks only need interpreted when investigating an infringement, so very little equipment needs to be watermark-aware at all. There are privacy concerns with tracking which digital media units correspond to which watermarks, but no more so than with other forms of tracking widely accepted. Consumers may be willing to trade this minor bit of privacy for better, cheaper equipment. This solution solves the problem of associating a unit ID with a wide-area digital broadcast, as well.

Another simple solution would be to add watermarks on the production end. The trust would reside in the correct place. Content owners would not rely on anyone else's diligence. This places no requirements on end consumer equipment at all, yielding great flexibility for both consumer and manufacturer ingenuity. The content owners can control their watermarking process entirely on their own with no need for ad-hoc standards between different content owners. Unfortunately, this does not solve the identification problems. Everyone receiving the same digital media stream will receive the same watermark. Hence, there are also no significant privacy concerns.

The last possibility that occurs to me is to add watermarks within the distribution network. This seems to combine many of the best features of the previous two. First, the primary trust relationship is between the content distribution network and the content owner. They already have significant trust relationships, so this allows re-use of existing business practices. Also, transparent

watermarking has no impact on the consumer's equipment. Because there are few interoperability issues, the watermarking standards can be driven by industry needs rather than government regulations. And consumers already have privacy trust relationships with their cable companies in regards to the services provided, so this adds few new privacy issues. Again, this solution would be difficult to implement usefully for wireless digital broadcasts, but it seems a perfect match for the particular context of *digital cable systems*.

Or at least it's a great match from the consumer's view. In many ways, it's also a great match for the content owners. Instead of holding many individuals responsible for correct use of the hardware involved, they can hold the distribution companies responsible. That should greatly ease their worries. For the content distributors, however, this is added cost. Many of the functions necessary to implement watermarking on a per-block or per-household level can be leveraged to provide other services, but the cost could present a significant short-term hurdle for digital cable adoption.

Watermarking in the distribution network appears the best long-term solution. It protects fair use, provides economic benefits to consumers and equipment manufacturers, fits into existing business and privacy practices, and protects content owners' rights. However, an FCC mandate requiring the currently proposed copy 'protection' scheme will undermine the market forces that will lead to the better long-term watermarking solution. The production and distribution sides will consider their jobs complete; they will be unwilling to invest significant effort in better solutions. In addition, consumers will be saddled with expensive hardware that will need to be replaced frequently to keep up with the latest minor changes in copy 'protection.' And the FCC will need to be involved in every minor change, increasing the taxpayer's burden and decreasing the FCC's effective work.

Because there are significant alternatives to the currently proposed copy 'protection' scheme, and because mandating that scheme will prevent exploration of the alternatives, I urge you not to mandate the proposed scheme.

Sincerely,

E. Jason Riedy

Submitted electonically. For verification of authenticity, mail `jason@acm.org` *or contact by phone at 510-841-4704.*